

Testimony of Michael Holden

Senior Counsel, Verizon Wireless

**Committee on Energy and Commerce
Subcommittee on Oversight and Investigations**

**Hearing on Internet Data Brokers and Pretexting:
Who Has Access to Your Private Records?**

September 29, 2006

Chairman Whitfield, Ranking Member Stupak, and members of the Subcommittee. I am Michael Holden, Senior Counsel from Verizon Wireless, and I thank you for the opportunity to appear before this Subcommittee to address your concerns about data pretexting. We should be clear on exactly what we are talking about. Terms like “pretexting” and “data brokers” mask the serious nature of the crimes being committed. We are talking about thieves who are perpetrating serious fraud, theft, and invasions of privacy.

I cannot emphasize enough how seriously Verizon Wireless takes the issue of consumer data theft and fraud. The protection of our more than 54 million customers’ private information is extremely important to us, and we are doing all we can to protect this data from thieves who seek to steal it. We obtain injunctions against data thieves. We team with law enforcement to prosecute data thieves. And we continually examine and implement improved safeguards to protect the information customers entrust to us.

Verizon Wireless Has Led the Fight Against Data Brokers and Pretexting

The best way to stop data fraudsters is to put them out of business. Individuals and entities that steal call records and other proprietary customer information should be

aggressively pursued and punished, which is why Verizon Wireless is leading the industry in efforts to find these con artists and shut them down.

To our knowledge, Verizon Wireless is the first private or public entity to take action on incidents of theft of cell phone records. We were the first to file lawsuits against individuals and companies who attempted to steal wireless customer information through pretexting. In July 2005, Verizon Wireless filed suit, believed to be the first of its kind, against Source Resources, Inc., a Tennessee company that advertised on its web site that it could obtain wireless telephone records and other confidential customer information. On September 13, 2005, Verizon Wireless obtained a permanent injunction against Source Resources.¹

Moreover, on November 2, 2005, Verizon Wireless obtained a temporary restraining order against Global Information Group (“GIG”), a Florida company which had made thousands of attempts to steal confidential information without proper authorization and used various fraudulent schemes to do so, including impersonating Verizon Wireless employees and posing as Verizon Wireless customers.² On June 28, 2006, the court entered a stipulated final judgment and permanent injunction against GIG. The injunction prohibits GIG from attempting to obtain customer information from any telecommunications provider, possessing or disclosing any customer information to third parties, and/or engaging in any form of pretexting against Verizon Wireless.

¹ *Cellco Partnership d/b/a Verizon Wireless v. Source Resources*, Permanent Injunction on Consent, Docket No. SOM-L-1013-05 (Sup. Ct. of N.J.; Law Div.: Somerset County, Sept. 13, 2005).

² *Cellco Partnership d/b/a Verizon Wireless v. Global Information Group, Inc., et al.*, Order, No. 05-09757 (Fla. Circuit Ct., 13th Judicial Circuit, Hillsborough County, Nov. 2, 2005).

On January 30, 2006, Verizon Wireless also won a preliminary injunction against Data Find Solutions, First Source Information Specialists, and related companies in U.S. District Court in Trenton, New Jersey.³ These companies are the current and former owners of the websites locatecell.com, celltolls.com, peoplesearchamerica.com, and datafind.org. These companies fraudulently attempted to obtain customer records by calling Verizon Wireless customer service centers and posing as Verizon Wireless employees needing access to confidential customer information. The injunction prohibits these fraudsters from attempting to obtain information on Verizon Wireless customers, providing any information on Verizon Wireless customers to any third parties, or operating any website that may advertise that they can obtain information on Verizon Wireless customers. This lawsuit is still pending.

Verizon Wireless issued press releases in conjunction with the filing of each of these lawsuits. These press releases served two goals -- they publicized the problem of data theft and they sent a message to data thieves that Verizon Wireless will pursue them through every legal means possible. In addition to these suits, Verizon Wireless has sent cease and desist letters to individuals operating data-theft operations and worked with law enforcement to pursue actions against data fraudsters.

Teaming with Law Enforcement and Government

Even before pretexting became front-page news, Verizon Wireless began teaming with law enforcement to identify individuals involved in fraudulent activities and put them out of business. For example, Verizon Wireless reached out to the Florida's

³ *Cellco Partnership d/b/a Verizon Wireless v. Data Find Solutions, Inc., et al.*, Order, No. 06-CV-326 (SRC) (D.N.J., Jan. 31, 2006).

Attorney General's ("AG") office with facts that enabled the state to bring its own lawsuits against GIG and First Source. Verizon Wireless has provided information and support to many law enforcement agencies and participated in conferences with law enforcement devoted to the topic of pretexting. Verizon Wireless also approached the FCC and briefed its staff members last year on its efforts to fight theft of personal data.

All of these efforts are effective because they target the wrongdoers, and focus on the methods used by fraudsters to illegally obtain confidential information. These efforts have made a difference. While the ongoing problem of pretexting should not be minimized, the combined efforts of Members of Congress, the FCC, the Federal Trade Commission, law enforcement officials, and carriers such as Verizon Wireless have put many data thieves out of business.

Internal Safeguards Protecting Confidential Customer Information

Verizon Wireless has always focused on the protection of customer information internally as well as externally. Verizon Wireless takes its customers' privacy very seriously and, beyond its legal obligations, it has every incentive to do so since a failure to impose adequate safeguards to protect that information will lead to a loss of customers, especially in the extremely competitive wireless marketplace. Verizon Wireless has always maintained internal safeguards and procedures for the use and disclosure of customer data, and it reviews those safeguards continually to determine whether modifications should be made. It is important to note, however, that Verizon Wireless handles well over 100 million calls to customer service each year, the vast majority of which are from actual customers with legitimate inquiries. Whatever measures we take

to protect against data thieves affects how legitimate calls are handled as well. With customer service a critical metric in our industry for customer satisfaction, we must be mindful of the overwhelming number of legitimate customer service inquiries we receive.

In response to the threat from pretexting, Verizon Wireless has taken a hard look at its safeguards, especially those designed to stop this deceitful activity in the manner in which it typically occurs. In most documented cases, data thieves have obtained confidential data through multiple fraudulent and deceptive phone calls to customer service. Some data fraudsters have also posed as customers to obtain online access to account information. Verizon Wireless is not aware of any cases in which data thieves were able to obtain such information through “hacking” into Verizon Wireless database systems or through a Verizon Wireless employee. There is also no evidence that our employees have been complicit in these schemes or are in any way involved with the thieves. Typically, fraudsters pose as Verizon Wireless employees, often providing customer service representatives (“CSRs”) with valid employee names and identification numbers. CSRs are thus on the front line in the fight against this problem. Thieves seek to capitalize on the natural inclination of CSRs to help customers resolve issues. They may also obtain certain customer information from other sources, and then use that information to obtain online access to a customer’s account.

Verizon Wireless has many safeguards to protect customer information from these threats. First, with respect to calls to customer service, no confidential customer information may be disclosed unless and until the CSR has fully verified the identity of the customer.

Second, certain information, such as social security number, credit card or checking account information, address, and unbilled call detail, cannot be disclosed to anyone, even the verified account holder.

Third, Verizon Wireless prohibits any faxing or e-mailing of cell phone records.

Fourth, training is paramount. Given that calls to customer service are fraudsters' main source of information, it is essential to educate CSRs to recognize pretexting and the particular methods that data thieves use in these scams. Although no system is 100 percent foolproof, Verizon Wireless has trained its employees, especially its CSRs, about the need to protect confidential information and the specifics of the pretexting techniques designed to dupe the representative into providing information.

In terms of formal training, Verizon Wireless maintains a comprehensive Code of Business Conduct (the "Code"). The Code prohibits the disclosure of confidential information unless the information must be produced pursuant to subpoena or other valid legal process. New hires are provided with a copy of the Code along with their offer letter. Verizon Wireless's Office of Integrity and Compliance ("OIC") has primary responsibility for drafting, disseminating, and training on the Code. It also maintains a confidential 800 number for employees to report possible violations of the Code, including violations related to customer privacy. Employees are advised of the 800 number via the Code, postings in the workplace, periodic e-mails, and an OIC brochure. The OIC brochure specifically instructs employees to report "misuse of confidential or proprietary information."

CSRs go through 5 ½ weeks of intensive, face-to-face training before they are put into the field. CSRs are trained on the Code during this initial training program, and must

also undergo online training on the Code each year. In addition, new hire training includes a session called “Servicing with Integrity,” which has specific sections, scenarios, and discussions regarding data thieves and pretexting.

Additional training relating to customer privacy, data brokers, or pretexting includes:

- “For Your Eyes Only,” an on-line module on privacy and pretexting that all employees were required to complete in September 2005.
- E-mail alerts to all employees on topics such as “Protecting Customer Data from Data Brokers.”
- Postings on the Verizon Wireless internal intranet site, “VZ Web.”
- Quarterly distribution to all employees of “Integrity Times,” a newsletter addressing ethics/compliance issues, including protection of confidential information and guarding against data theft.
- Written Methods & Procedures for CSRs and marketing personnel, detailing required procedures for identifying and verifying subscribers and protecting confidential information (updated August 4, 2006).
- Written Methods & Procedures for handling suspected pretexting calls (updated January 19, 2006).
- Flash updates and reminders regarding pretexting methods and customer privacy.

Fifth, if a customer wants extra layers of protection beyond typical verification procedures, that customer can establish a “billing system passcode.” If such a passcode is established for an account, that passcode must be provided before any account information is disclosed, either by customer service or in-store personnel. Moreover, if a subscriber sets up a billing system passcode on his or her account, he or she must also input that passcode to obtain online access.

Sixth, Verizon Wireless is committed to protecting the integrity of its systems that provide online access to account information. Customers can manage their accounts and

access certain account information online, but cannot access other personally identifiable information, such as social security numbers or usable credit or bank account information. A user cannot establish or access an account online unless and until he or she provides the information necessary to verify the subscriber.

In March 2006, Verizon Wireless enhanced the security procedures associated with online access to an account. Now, in addition to the data that is normally required to verify the customer, whenever an online account is established or a customer forgets the password, a temporary password is sent to the customer's wireless phone by text message (or by letter if the phone cannot receive text messages) and that password must be input into the website to gain access. Moreover, a "challenge question" (e.g., who was your favorite high school teacher?) is associated with online accounts, and this question will be asked if the customer forgets the password.

Conclusion

Data thieves and fraudsters prey on the instinct of CSRs and wireless carriers to help customers and provide the best possible customer service. Indeed, what was good customer service yesterday may now be viewed as a potential security flaw. That is why Verizon Wireless has gone to such great lengths to educate its CSRs about data theft and to improve the security of its online systems. And that is also why we need to take aggressive offensive actions against the data thieves. We will continue to aggressively pursue these data thieves through our internal security processes, partner with state and federal law enforcement and regulators, and do everything we can to protect our more than 54 million customers' information from unauthorized review. In the end, our

challenge is to screen out the relatively few pretexting calls to customer service, while providing the best customer service to the over 100 million legitimate calls we receive each year.

We share your concerns about this problem, and are doing all that we can each day to prevent these thieves from stealing our customer data. Thank you for the opportunity to appear before you today, and I will be happy to answer any questions you may have.